UTM MACHINE IN 3-1/2 INCH FLOPPY DISK CASE

Relation to Previous Application

This application is a continuation-in-part of application U.S. Pat. App. Serial No. 09/322,669 filed on May 28, 1999.

Cross Reference to Related Applications:

This application is related to UNIVERSAL TELLER MACHINE, U.S. Pat. App. Serial No. 09/322,670, filed on May 28, 1999, and THIN MAGNETIC MEDIUM READ HEAD, U.S. Pat. App. Serial No. 9/560,842 filed April 28, 2000, which are incorporated by reference.

Technical Field:

The invention relates generally to electronic devices, and more particularly to a UTM machine that can be inserted into a computer's 3-1/2 inch disk drive.

Background of the Invention:

Credit cards and debit cards have magnetic stripes that contain the cardholder's personal information; *e.g.,* name and card account number. There are readers for reading the magnetic stripes at many retail point-of-sale locations. Debit cards can be used at these locations by swiping the card through the reader and entering a personal identification number (PIN) into the reader's keypad. Adequate security is achieved by a secure communications connection between the reader and a remote computer/server and by the cardholder possessing a debit card that can be read by the reader and knowing the PIN associated with the card. Credit cards can be used at these same locations by the cardholder signing a document for comparison by a clerk to a signature on the back of the card. Adequate security is achieved by the cardholder possessing a card that appears to the clerk to be authentic and being able to produce a signature that matches the signature on the back of the card.

For Internet financial transactions, the above-described security features are not available for credit cards and debit cards. There is no retail clerk to verify that

the card looks authentic and to compare the cardholder's signature with the signature on the back of the card. There also is no secure communications connection between a card reader that is connected to the user's host computer and the remote computer/server. Solutions to these problems should greatly expand Internet commerce.

Various companies, including IBM, Hewlett-Packard, Intel, and Wave have proposed solving this problem by including a "smart chip" in each personal computer. The smart chip stores a unique identification code that cannot be read but which can be used with encryption to prove the identification of the chip to a remote computer/server across a communications line. Thus, encryption of this code provides a secure identification of the computer. Presumably, the owner of the host computer can be held responsible for its use. Entry of a PIN at a keyboard connected to the host computer may also be required. With the ability to prove which host computer placed a communication for a financial transaction and that a particular PIN was used, adequate security will be achieved for many financial transactions.

Other companies have proposed the use of smart cards placed in a smart-card reader at each host computer. Each smart card would include a smart chip as described above. The smart card is guarded by its owner like a key. The person who possesses the smart card is presumed to be its proper owner. Entry of a PIN at a keyboard connected to the host computer to which the smart card reader is also connected can also be required. With the ability to prove which smart card was used for a financial transaction and that the PIN associated with the smart card was also used, adequate security will be achieved for many financial transactions.

SUMMARY OF THE INVENTION

The invention is a universal teller machine ("UTM") adapted to a case for a 3-1/2-inch floppy-disk with means for communicating to a personal computer through a standard 3-1/2-inch floppy-disk drive.

In one aspect of the invention, an electronic device includes a 3-1/2-inch floppy-disk shaped housing with a slot, a thin magnetic read head, a disk drive communications transducer, and a processing circuit disposed within the housing. The slot receives a card having a magnetic stripe that stores information, and the

magnetic read head reads the information stored on the stripe. The processing circuit receives the information read by the read head and provides processed information to the transducer.

In another aspect of the invention, the processing circuit includes a smart chip for performing security functions which provides a unique identification code to the transducer. The smart chip is contained in a removable SIM (Subscriber Identification Module) which inserted into a SIM port within the device. Alternatively, the smart chip may be embedded in the device. For purposes of this discussion, a smart chip includes security circuitry that can facilitate security functions, such as authentication, encryption and decryption, digital signatures, unique identification code storage and other well known smart chip functions. In the present invention the smart chip provides authentication to a remote server across a network by confirming a unique identification to the remote server without revealing to the local computer or any intervening device in the communications link enough information that, if captured, can be used to imitate the smart chip.

Another aspect of the invention provides for direct input of user known information, such as a PIN, via a keypad on the surface of the device. This allows the PIN to be entered into the smart chip without being transmitted to the PC where it could be intercepted by unauthorized software running on the PC.

Communications between the device and the user, such as prompts and process confirmations for instance, are provided via a display, such as a liquid crystal display (LCD) or an LED array, and/or audible means such as a tone or speech generator.

Thus, such a device can receive encoded information from a magnetic stripe on a card and/or user known information, such as a PIN, and it can be inserted into a host computer to communicate with the host computer via the computer's floppy-disk drive. Such a device eliminates the need for special connections to the host computer. Additionally, the device can ensure the security of a credit/debit card transaction by using the secure authentication features of the smart chip and requiring a personal identification number (PIN) or other user information that identifies the cardholder. Also, the device can generate user authentication tokens for use in other types of transactions and online activities such as on-line stock trading, accessing confidential databases or generating digital signatures.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a front view of the UTM machine.

Figure 2 is a schematic block diagram of the circuitry of the card reader of Figure 1.

Figure 3 is a perspective view of the very thin magnetic-stripe read head according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Overview:

Generally, the various aspects and embodiments of the invention provide security for internet credit/debit card transactions and other activities requiring user authentication, and the following description is a general overview of one of these embodiments The user of the UTM machine is uniquely identified by a removable SIM inserted into a SIM port within the UTM machine and each SIM is associated with a person or with a credit/debit card or other card bearing magnetically encoded information thereon (hereinafter, "card"). SIMs are well known in the electronics industry. As is the case in the present invention, SIM's often include "smart chip" circuitry that can process information and store values. Smart chips are adaptable to a wide variety of devices and shapes, but they are commonly found in a "smart card" which typically has a form factor similar to a credit card. Alternatively, the smart chip can be embedded within the device rather than inserted into a socket where it is removable. In the discussion below, each reference to smart chip should be understood as a reference to an embedded smart chip or to a removable smart chip within a SIM or within another type of carrier such as a smart card. Additional security is provided in the case of SIMs, smart cards or embedded smart chips that require entry of a PIN before the processing can be continue. For purposes of this discussion a PIN is synonymous with user information that is used to identify the user. The user information may be a numeric sequence, such as a typical PIN, a combination of numbers and/or other symbols, or a fingerprint or other bio-metric data.

The unique identification code of the smart chip is registered on a remote central computer/server in association with accurate identification of the cardholder

to whom the SIM or device with embedded smart chip was issued. Using a secure PIN entered via a keypad on the UTM machine, that cardholder can create a list of credit and debit cards that are authorized for use with the reader. The list can be stored in secure memory in the smart chip or on the remote central computer/server. When the cardholder swipes a card through the reader, the identifying information read from the card is transmitted from the device to a host computer then to a central computer/server where it is compared with the corresponding information on the central computer/server associated with the unique identification code stored in the smart chip. If the identifying information and code do not match, then the transaction may be disallowed for inadequate security.

The UTM machine in a 3-1/2-inch floppy-disk housing is portable and easily connected to or disconnected from the cardholder's computer or any other host computer. This allows the cardholder to easily guard his/her possession of the UTM machine and to permit others to use his/her computer without a security risk. Also, if the smart chip is in a removable SIM, the SIM can also be removed and stored in a secure location to provide greater security.

Additional security is provided by the fact that the smart chip being external to the host computer makes the information stored on it less accessible to hacker software. Also, by entering the PIN external to the host computer, a hacker program residing on the host computer to record keystrokes or similar eavesdropping programs cannot intercept an unencrypted PIN.

Typically, the UTM machine will be issued with a particular credit/debit card account or user access account in mind. However, since the SIM is removable, the UTM machine can be used with another combination of SIM and card. Alternatively, a single SIM may be associated with several cards issued by different institutions through a cooperative arrangement.

Unlike many ATMs, neither the smart chip in the card reader nor the cardholder's computer will attempt to decrypt the cardholder's PIN from encrypted information on the card if such information is present. Placing this decryption information in every reader or in software distributed with each reader presents a security risk. Instead, for use with debit cards for example, the PIN is transmitted from the reader keypad to the smart chip where it is verified. The smart chip features make it impossible to extract or decode the process by which the PIN is

verified. Alternatively, the user enters the PIN for the debit card, and the PIN is encrypted through the use of the smart chip and transmitted to the remote computer/server, along with the encrypted unique identification code stored on the smart chip, for comparison with the PIN stored on the remote computer/server as corresponding to the identification code.

Because the UTM machine includes a smart chip, the smart chip may be used for other familiar smart chip functions such as storing electronic cash. The cardholder who owns the UTM machine can swipe a credit/debit card and download electronic cash into the smart chip for use in transactions that are for very small amounts of money, where transaction fees or delays are unacceptable, or for use in anonymous transactions. Alternatively, because the smart chip is in a SIM, the cardholder can give the SIM, or the SIM and UTM machine to another person without providing the cardholder's credit/debit card, and that other person can then spend the electronic cash stored in the smart chip without having access to the cardholder's credit/debit card accounts.

Device Structure & Operation:

Figure 1 is a front view with of a UTM machine 10 according to an embodiment of the invention. The UTM machine 10 includes a housing 12 designed to standard floppy-disk specifications sufficient to allow the UTM machine 10 to be inserted into and communicate with a conventional floppy-disk drive without damaging the drive or requiring modification of the drive. The UTM machine 10 includes a slot 14 for receiving a card 16, which has a magnetic stripe 18 for storing cardholder information (*e.g.,* bank account number or other identifying information). A switch 20 functions as a power switch to activate the UTM machine prior to the card 16 being swiped through the slot 14. Alternatively, the switch 20 may be a mechanical switch or an optical switch internal to the UTM machine that senses the presence of the card 16 in the slot 14, which then energizes the internal circuitry.

An encoded information read head 22 (hereinafter "read head") reads the information encoded on the magnetic stripe 18 as the card is swiped through the slot 14 in the direction indicated 23. The encoded information may be in a form other than magnetically encoded data. For instance, the information may be optically encoded such as in a bar code, and the read head would be of a type capable of

reading optically encoded information. The UTM machine 10 includes a SIM port 27 for receiving a removable SIM 28, which is associated with an owner or a particular card or set of cards. The SIM 28 also performs typical smart chip encryption and authentication. It may also perform other smart chip functions such as value storage. A disk drive communications transducer 30 (hereinafter "transducer") on the backside of the UTM machine 10 allows it to communicate with the read/write head (not shown) of a conventional floppy-disk drive by mimicking the electrical signals the read/write head would normally expect when communicating with a conventional floppy disk. The transducer 30 may be referred to as a "communications head" for instance, or something similar, but it is intended herein to refer to any device or circuit incorporated in the UTM machine 10 that can communicate with the read/write head of a typical floppy-disk drive. A conventional battery 32 supplies power to the device. A display 36 may indicate battery power level, user prompts, function and status messages. The UTM machine 10 has a keypad 37 used to enter PIN codes, respond to various prompts, initiate authentication, select transaction types and to launch host computer based applications once the UTM machine has been inserted in the floppy-disk drive.

The SIM 28 is preferably programmed for dual key (public/private) encryption such as for use with the secure electronic transactions (SET) protocol. The SIM 28 may include electronic-key circuitry that is capable of securely encrypting a unique identifier and transmitting it to a remote computer/server such as with DES encryption or another encryption protocol such as RSA.

An alternative embodiment includes Braille symbols on the keypad and audible responses, prompts, and status messages so persons with impaired vision may use the UTM machine.

Figure 2 is a schematic block diagram of a processing circuit 44 for the UTM machine 10 of Figure 1. According to an embodiment of the invention magnetic-stripe read circuitry 50 includes the thin read head 22 which reads the magnetically encoded data from the magnetic stripe 18 (ref. Figure 1) and converts it into a digital signal. The magnetic-stripe read circuitry is coupled to the programmable logic 49. A microcontroller 48 is coupled to the SIM port 27, the display 36, the power supply and the programmable logic 49. The microcontroller 48 receives the magnetic-stripe information from the programmable logic 49 and the identification code from a SIM

28 inserted in SIM port 27 and provides them after processing to the programmable logic 49 which is coupled to an electromagnetic interface circuit 52, which includes the transducer 30. The floppy drive interface circuit 52 converts this information into a signal that can be read by a floppy-disk drive read/write head 41 and transmits this signal to the transducer 30. The programmable logic is also coupled to the keypad circuitry 53, which includes keypad 37. A conventional power supply 54, including the battery 32, supplies power to all of the processing circuitry 44 and the SIM. Memory 55 is coupled to programmable logic 49, which passes information from the memory 55 to the microcontroller 48 as needed. An alternative embodiment incorporates microcontroller 48, programmable logic 49 and memory 55 in an application specific integrated circuit (ASIC) 100. Another alternative embodiment takes advantage of the processing capabilities of SIM's to reduce the complexity of the circuitry and perform microcontroller functions in the SIM rather than having a sophisticated processing circuit built into the UTM machine.

Referring to Figures 1 and 2, to use the UTM machine 10, a cardholder inserts the SIM 28 in the SIM port 27, activates the power switch 20 and swipes his card 16 through the slot 14. As the magnetic stripe 18 moves by the read head 22, the read head 22 senses the magnetically encoded information on the stripe 18 and converts this information into electrical signals. The read circuitry 50 then converts these electrical signals into a digital signal that represents the stored information and provides this digital signal to the programmable logic 49. After the microcontroller 48 receives and stores the magnetic-stripe information, it causes the display 36 to indicate that the reading of the stripe 18 was successful. Alternatively, if there was a read error, the microcontroller 48 causes the display 36 to generate a prompt to indicate to the cardholder that he needs to re-swipe the card 16 through the slot 14. In addition, if the transaction requires a PIN, the cardholder is prompted to enter his PIN on the keypad 37.

Once the cardholder has swiped the card 16 through the slot 14 and the display 36 indicates proper reading of the magnetic-stripe and SIM information, the cardholder inserts the UTM machine into a floppy-disk drive. Once the UTM machine 10 is inserted in the disk drive, the UTM machine provides the SIM information, the information read from the magnetic stripe 18, and PIN information if required, to a remote computer/server (not shown) via the communications circuitry

52, the disk drive read/write head 41, and the host computer in which the disk drive is installed (not shown). The host computer provides additional information (*e.g.*, items to be purchased) regarding the transaction that the cardholder enters via a keyboard, mouse, or other means.

In one embodiment, the SIM 28 encrypts the identification code and magnetic-stripe information according to conventional encryption techniques. Alternatively, the identification code may be stored in encrypted form on the SIM 28 or the information may be stored in encrypted form on the magnetic stripe. In such a case, the microcontroller 48 does not alter the code or the magnetic-stripe information before sending it to the remote computer/server.

The UTM machine also has a time out function. Once the requisite actions have been taken, such as card swiping and PIN entry, the device will time out and clear its memory of magnetic stripe information and the PIN if it is not inserted in a computer and/or the transaction is not commanded to proceed within a pre-defined time limit. This feature adds additional security by preventing an unauthorized user from successfully using the UTM machine after the owner of the UTM machine has entered his information.

Figure 3 is a perspective view of the magnetic-stripe read head 22 of Figure 1 according to an embodiment of the invention. The read head 22 is thin enough for placement within the floppy-disk housing 12 of Figure 1. This embodiment of the read head 22 is discussed in detail in patent application THIN MAGNETIC MEDIUM READ HEAD, U.S. Pat. App. Serial No. 9/560,842 filed April 28, 2000 and which is incorporated by reference.

An error free read of a magnetic stripe typically requires four to eight ounces of contact pressure between the read head and the magnetic stripe. The UTM machine housing may require additional integral stiffening if it is molded of conventional plastics so that the portions of the housing forming the slot will provide sufficient pressure between the read head and the card as a card is swiped through it. Alternatively, metallic forms may be added to stiffen the housing or provide a biasing force that aids in squeezing the read head against the card. Occasionally a card is bent due to being stored in a wallet. Accordingly, the housing can be made to allow a portion of it to subtly rotate or pivot relative to the remainder of the housing forming the slot so the read head maintains optimum contact with a bent card as the

card passes by it. Alternatively, the read head can be suspended in a carrier element that will allow it to rotate as described above.

From the foregoing it will be appreciated that, although specific embodiments of the invention have been described herein for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention.